Amendments to the Claims

Claim 1 (currently amended): A computer program product for enabling a subsequent user sign-on during a certificate-based host access session, said computer program product embodied on a computer-readable medium and comprising:

computer-readable program code means for processing a first sign-on during a secure session using a digital certificate, further comprising:

computer-readable program code means for establishing said secure session from a client machine to a server machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

computer-readable program code means for storing said digital certificate or a reference thereto at said server machine;

computer-readable program code means for establishing a session from said server machine to a host system using a legacy host communication protocol, responsive to receiving, at said server machine, a first sign-on request from said client machine, wherein said first sign-on request identifies a first secure legacy host application to which said first sign-on is requested;

computer-readable program code means for passing said stored digital certificate or said reference from said server machine to a host access security system;

computer-readable program code means, operable in said host access security system, for authenticating said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

computer-readable program code means, operable in said host access security system, for using said passed or retrieved digital certificate to locate access credentials for said

user;

computer-readable program code means, operable in said host access security system, for accessing a stored password or generating a password substitute representing said located credentials;

computer-readable program code means, operable in said host access security system, for returning said stored password or generated password substitute to said server machine, along with a first user identifier corresponding to said located credentials;

computer-readable program code means, operable in said server machine, for receiving a first sign-on message from said client machine, wherein said first sign-on message uses placeholder syntax, said placeholder syntax representing a user identification and a password of said user, wherein said user identification and said password are expected in said first sign-on message by said first secure legacy host application; and

computer-readable program code means, operable in said server machine, for using said returned password or password substitute and said returned first user identifier to transparently complete said first sign-on, on behalf of said user of said client machine, to said first secure legacy host application executing at said host system by substituting said returned first user identifier and said returned password or password substitute for said placeholder syntax in said first sign-on message, thereby creating a revised first sign-on message, and forwarding said revised first sign-on message from said server machine to said first secure legacy host application; and

computer-readable program code means for processing a subsequent sign-on of said user during said secure session using said digital certificate, further comprising:

computer-readable program code means for receiving a subsequent sign-on request, at said server machine from said client machine, wherein: (1) said subsequent sign-on request identifies a second secure legacy host application to which said subsequent sign-on is requested; (2) said subsequent sign-on requires authenticating a requester of said subsequent sign-on; (3) said second secure legacy host application may be identical to said first secure legacy host application; and (4) said requester of said subsequent sign-on is said user;

computer-readable program code means, operable at said server machine, for retrieving said stored digital certificate or reference;

computer-readable program code means for passing said retrieved digital certificate or reference from said server machine to said host access security system;

computer-readable program code means, operable in said host access security system, for re-authenticating said identity of said user, thereby authenticating said requester, using said passed retrieved digital certificate or retrieved reference;

computer-readable program code means, operable in said host access security system, for using said passed retrieved digital certificate or retrieved reference to [[again]] re-locate said access credentials for said user;

computer-readable program code means, operable in said host access security system, for re-accessing said stored password or generating a new password substitute representing said re-located credentials;

computer-readable program code means, operable in said host access security system, for returning said re-accessed stored password or generated new password substitute to said server machine, along with said user identifier corresponding to said re-located credentials;

and

computer-readable program code means, operable in said server machine, for using said returned re-accessed password or new password substitute and said returned user identifier corresponding to said re-located credentials to transparently complete said subsequent sign-on, on behalf of said requester, to said second secure legacy host application executing at said host system.

Claim 2 (currently amended): The computer program product as claimed in Claim 1, wherein said digital certificate ~~and said second digital certificate are~~ is an X.509 certificate ~~certificates~~ and said digital certificate reference is a reference to an X.509 certificate.

Claim 3 (original): The computer program product as claimed in Claim 1, wherein said communication protocol is a 3270 emulation protocol.

Claim 4 (original): The computer program product as claimed in Claim 1, wherein said communication protocol is a 5250 emulation protocol.

Claim 5 (original): The computer program product as claimed in Claim 1, wherein said communication protocol is a Virtual Terminal protocol.

Claim 6 (original): The computer program product as claimed in Claim 3, wherein said host access security system is a Resource Access Control Facility (RACF) system.

Claim 7 (original): The computer program product as claimed in Claim 1, wherein said server machine is a Web application server machine.

Claim 8 (canceled)

Claim 9 (previously presented): The computer program product as claimed in Claim 7, wherein:

said computer-readable program code means for using said returned password or password substitute and said returned first user identifier to transparently complete said first sign-on further comprises:

computer-readable program code means for requesting by said first secure legacy host application, responsive to said computer-readable program code means for establishing said session, first sign-on information for said user; and

computer-readable program code means for responding to said request for first sign-on information by supplying, from said server machine to said first secure legacy host application, said returned user identifier and said returned password or password substitute.

Claim 10 (currently amended): A system for enabling a subsequent user sign-on during a certificate-based host access session, comprising:

means for processing a first sign-on during a secure session using a digital certificate, further comprising:

means for establishing said secure session from a client machine to a server

machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

means for storing said digital certificate or a reference thereto at said server machine;

means for establishing a session from said server machine to a host system using a legacy host communication protocol, responsive to receiving, at said server machine, a first sign-on request from said client machine, wherein said first sign-on request identifies a first secure legacy host application to which said first sign-on is requested;

means for passing said stored digital certificate or said reference from said server machine to a host access security system;

means, operable in said host access security system, for authenticating said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

means, operable in said host access security system, for using said passed or retrieved digital certificate to locate access credentials for said user;

means, operable in said host access security system, for accessing a stored password or generating a password substitute representing said located credentials;

means, operable in said host access security system, for returning said stored password or generated password substitute to said server machine, along with a first user identifier corresponding to said located credentials;

means, operable in said server machine, for receiving a first sign-on message from said client machine, wherein said first sign-on message uses placeholder syntax, said placeholder

syntax representing a user identification and a password of said user, wherein said user identification and said password are expected in said first sign-on message by said first secure legacy host application; and

means, operable in said server machine, for using said returned password or password substitute and said returned first user identifier to transparently complete said first sign-on, on behalf of said user of said client machine, to said first secure legacy host application executing at said host system by substituting said returned first user identifier and said returned password or password substitute for said placeholder syntax in said first sign-on message, thereby creating a revised first sign-on message, and forwarding said revised first sign-on message from said server machine to said first secure legacy host application; and

means for processing a subsequent sign-on of said user during said secure session using said digital certificate, further comprising:

means for receiving a subsequent sign-on request, at said server machine from said client machine, wherein: (1) said subsequent sign-on request identifies a second secure legacy host application to which said subsequent sign-on is requested; (2) said subsequent sign-on requires authenticating a requester of said subsequent sign-on; (3) said second secure legacy host application may be identical to said first secure legacy host application; and (4) said requester of said subsequent sign-on is said user;

means, operable at said server machine, for retrieving said stored digital certificate or reference;

means for passing said retrieved digital certificate or reference from said server machine to said host access security system;

means, operable in said host access security system, for re-authenticating said identity of said user, thereby authenticating said requester, using said passed retrieved digital certificate or retrieved reference;

means, operable in said host access security system, for using said passed retrieved digital certificate or retrieved reference to [[again]] re-locate said access credentials for said user;

means, operable in said host access security system, for re-accessing said stored password or generating a new password substitute representing said re-located credentials;

means, operable in said host access security system, for returning said re-accessed stored password or generated new password substitute to said server machine, along with said user identifier corresponding to said re-located credentials; and

means, operable in said server machine, for using said returned re-accessed password or new password substitute and said returned user identifier corresponding to said re-located credentials to transparently complete said subsequent sign-on, on behalf of said requester, to said second secure legacy host application executing at said host system.

Claim 11 (currently amended): The system as claimed in Claim 10, wherein said digital certificate ~~and said second digital certificate are~~ is an X.509 ~~certificates~~ certificate and said digital certificate reference is a reference to an X.509 certificate.

Claim 12 (original): The system as claimed in Claim 10, wherein said communication protocol is a 3270 emulation protocol.

Claim 13 (original): The system as claimed in Claim 12, wherein said host access security system is a Resource Access Control Facility (RACF) system.

Claim 14 (original): The system as claimed in Claim 10, wherein said server machine is a Web application server machine.

Claim 15 (canceled)

Claim 16 (previously presented): The system as claimed in Claim 14, wherein:

said means for using said returned password or password substitute and said returned first user identifier to transparently complete said first sign-on further comprises:

means for requesting by said first secure legacy host application, responsive to said means for establishing said session, first sign-on information for said user; and

means for responding to said request for first sign-on information by supplying, from said server machine to said first secure legacy host application, said returned user identifier and said returned password or password substitute.

Claim 17 (currently amended): A method for enabling a subsequent user sign-on during a certificate-based host access session, comprising the steps of:

processing a first sign-on during a secure session using a digital certificate, further comprising the steps of:

establishing said secure session from a client machine to a server machine using

said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

storing said digital certificate or a reference thereto at said server machine;

establishing a session from said server machine to a host system using a legacy host communication protocol, responsive to receiving, at said server machine, a first sign-on request from said client machine, wherein said first sign-on request identifies a first secure legacy host application to which said first sign-on is requested;

passing said stored digital certificate or said reference from said server machine to a host access security system;

authenticating, by said host access security system, said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

using, by said host access security system, said passed or retrieved digital certificate to locate access credentials for said user;

accessing, by said host access security system, a stored password or generating a password substitute representing said located credentials;

returning, by said host access security system, said stored password or generated password substitute to said server machine, along with a first user identifier corresponding to said located credentials;

receiving, by said server machine, a first sign-on message from said client machine, wherein said first sign-on message uses placeholder syntax, said placeholder syntax representing a user identification and a password of said user, wherein said user identification and said password are expected in said first sign-on message by said first secure legacy host application; and

using, by said server machine, said returned password or password substitute and said returned first user identifier to transparently complete said first sign-on, on behalf of said user of said client machine, to said first secure legacy host application executing at said host system by substituting said returned first user identifier and said returned password or password substitute for said placeholder syntax in said first sign-on message, thereby creating a revised first sign-on message, and forwarding said revised first sign-on message from said server machine to said first secure legacy host application; and

processing a subsequent sign-on of said user during said secure session using said digital certificate, further comprising the steps of:

receiving a subsequent sign-on request, at said server machine from said client machine, wherein: (1) said subsequent sign-on request identifies a second secure legacy host application to which said subsequent sign-on is requested; (2) said subsequent sign-on requires authenticating a requester of said subsequent sign-on; (3) said second secure legacy host application may be identical to said first secure legacy host application; and (4) said requester of said subsequent sign-on is said user;

retrieving, by said server machine, said stored digital certificate or reference;

passing said retrieved digital certificate or reference from said server machine to said host access security system;

re-authenticating, by said host access security system, said identity of said user, thereby authenticating said requester, using said passed retrieved digital certificate or retrieved reference;

using, by said host access security system, said passed retrieved digital certificate

or retrieved reference to [[again]] re-locate said access credentials for said user;

re-accessing, by said host access security system, said stored password or generating a new password substitute representing said re-located credentials;

returning, by said host access security system, said re-accessed stored password or generated new password substitute to said server machine, along with said user identifier corresponding to said re-located credentials; and

using, by said server machine, said returned re-accessed password or new password substitute and said returned user identifier corresponding to said re-located credentials to transparently complete said subsequent sign-on, on behalf of said requester, to said second secure legacy host application executing at said host system.

Claim 18 (currently amended): The method as claimed in Claim 17, wherein said digital certificate ~~and said second digital certificate are~~ is an X.509 ~~certificates~~ certificate and said digital certificate reference is a reference to an X.509 certificate.

Claim 19 (original): The method as claimed in Claim 17, wherein said communication protocol is a 3270 emulation protocol.

Claim 20 (original): The method as claimed in Claim 19, wherein said host access security system is a Resource Access Control Facility (RACF) system.

Claim 21 (original): The method as claimed in Claim 17, wherein said server machine is a Web

application server machine.

Claim 22 (canceled)

Claim 23 (previously presented): The method as claimed in Claim 21, wherein:

said step of using said returned password or password substitute and said returned first user identifier to transparently complete said first sign-on further comprises the steps of:

requesting by said first secure legacy host application, responsive to said step of establishing said session, first sign-on information for said user; and

responding to said request for first sign-on information by supplying, from said server machine to said first secure legacy host application, said returned user identifier and said returned password or password substitute.

Claim 24 (currently amended): The computer program product as claimed in Claim 1, wherein:

said computer-readable program code means for processing said subsequent sign-on further comprises:

computer-readable program code means for requesting, by said second secure legacy host application, subsequent sign-on information for said requester; and

computer-readable program code means for responding to said request for subsequent sign-on information by sending a subsequent sign-on message with placeholders from said client machine to said server machine, said placeholders representing said user identification and said password of said user; and

said computer-readable program code means for using said returned re-accessed password or new password substitute and said returned user identifier corresponding to said re-located credentials to transparently complete said second sign-on further comprises:

computer-readable program code means for substituting said returned user identifier corresponding to said re-located credentials and said returned re-accessed password or new password substitute for said placeholders in said subsequent sign-on message, thereby creating a revised subsequent sign-on message; and

computer-readable program code means for forwarding said revised subsequent sign-on message from said server machine to said second [[sure]] secure legacy host application.

Claim 25 (previously presented): The computer program product as claimed in Claim 7, wherein said computer-readable program code means for processing said subsequent sign-on further comprises:

computer-readable program code means for requesting, by said second secure legacy host application, subsequent sign-on information for said requester; and

computer-readable program code means for responding to said request for subsequent sign-on information by supplying, from said server machine to said second secure legacy host application, said returned user identifier associated with said re-located credentials and said returned re-accessed password or new password substitute.

Claim 26 (currently amended): The system as claimed in Claim 10, wherein:

said means for processing said subsequent sign-on further comprises:

means for requesting, by said second secure legacy host application, subsequent sign-on information for said requester; and

means for responding to said request for subsequent sign-on information by sending a subsequent sign-on message with placeholders from said client machine to said server machine, said placeholders representing said user identification and said password of said user; and

said means for using said returned re-accessed password or new password substitute and said returned user identifier corresponding to said re-located credentials to transparently complete said second sign-on further comprises:

means for substituting said returned user identifier corresponding to said re-located credentials and said returned re-accessed password or new password substitute for said placeholders in said subsequent sign-on message, thereby creating a revised subsequent sign-on message; and

means for forwarding said revised subsequent sign-on message from said server machine to said second [[sure]] secure legacy host application.

Claim 27 (previously presented): The system as claimed in Claim 14, wherein said means for processing said subsequent sign-on further comprises:

means for requesting, by said second secure legacy host application, subsequent sign-on information for said requester; and

means for responding to said request for subsequent sign-on information by supplying, from said server machine to said second secure legacy host application, said returned user

identifier associated with said re-located credentials and said returned re-accessed password or new password substitute.

Claim 28 (currently amended): The method as claimed in Claim 17, wherein:

said step of processing said subsequent sign-on further comprises the steps of:

requesting, by said second secure legacy host application, subsequent sign-on information for said requester; and

responding to said request for subsequent sign-on information by sending a subsequent sign-on message with placeholders from said client machine to said server machine, said placeholders representing said user identification and said password of said user; and

said step of using said returned re-accessed password or new password substitute and said returned user identifier corresponding to said re-located credentials to transparently complete said second sign-on further comprises the steps of:

substituting said returned user identifier corresponding to said re-located credentials and said returned re-accessed password or new password substitute for said placeholders in said subsequent sign-on message, thereby creating a revised subsequent sign-on message; and

forwarding said revised subsequent sign-on message from said server machine to said second [[sure]] secure legacy host application.

Claim 29 (previously presented): The method as claimed in Claim 21, wherein said step of processing said subsequent sign-on further comprises the steps of:

requesting, by said second secure legacy host application, subsequent sign-on information for said requester; and

responding to said request for subsequent sign-on information by supplying, from said server machine to said second secure legacy host application, said returned user identifier associated with said re-located credentials and said returned re-accessed password or new password substitute.

Claim 30 (currently amended): A computer-implemented method for enabling an identity to be subsequently provided during a certificate-based host access session, comprising steps of:

establishing a secure session between a client and a server using a digital certificate owned by a user of said client;

remembering said digital certificate at said server;

completing a first sign-on to a host application, by said server on behalf of said user, responsive to receiving an asynchronous sign-on request from said client that identifies said host application, further comprising the steps of:

using said remembered digital certificate to authenticate said user to a host access security component;

if said user is authenticated, locating, by said host access security component, access credentials of said user;

creating, by said host access security component, a passticket that represents said located access credentials;

returning said passticket from said host access security component to said server,

along with a user identifier associated with said located access credentials; and

inserting, by said server, said passticket and said user identifier into a log-on message in place of placeholders ~~therefor~~ for a user password and said user identifier, when said log-on message is received at said server from said client, thereby creating a revised log-on message, in a form expected by said host application, that is then sent from said server to sign said user on to said host application; and

completing a subsequent sign-on to a second host application, by said server on behalf of said user, responsive to receiving a second asynchronous sign-on request from said client that identifies said second host application, wherein said second host application may be identical to said host application, further comprising the steps of:

passing said remembered digital certificate from said server to said host access security component for authenticating said user for access to said second host application;

if said user is authenticated for access to said second host application, locating, by said host access security component, second access credentials of said user, wherein said second access credentials may be identical to said located access credentials;

creating, by said host access security component, a second passticket that represents said located second access credentials of said user;

returning said second passticket from said host access security component to said server, along with a second user identifier associated with said second located access credentials; and

inserting said returned second passticket and said returned second user identifier into a subsequent log-on message in place of placeholders for a second user password and said

second user identifier, when said second log-on message is received at said server from said client, thereby creating a second revised log-on message, in said form expected by said second host application, that is then sent from said server to sign said user on to said second host application.

Claim 31 (new): A method of providing subsequent user identification during a secure session, comprising steps of:

upon receiving a first log-on message containing placeholder syntax from a client during a secure session, substituting therefor a user identifier and a first password substitute provided by a host access security system upon authentication of user credentials associated with the client and with a user thereof, thereby creating a revised first log-on message in a form expected by a first legacy host application, the first password substitute representing access privileges associated with the user credentials for the first legacy host application;

forwarding the revised first log-on message to the first legacy host application for completing a secure sign-on thereto;

upon receiving a second log-on message containing placeholder syntax from the client during the secure session, substituting therefor the user identifier and a second password substitute provided by the host access security system upon authentication of the user credentials associated with the client and with the user thereof, thereby creating a revised second log-on message in a form expected by a second legacy host application, the second password substitute representing access privileges associated with the user credentials for the second legacy host application, wherein the second legacy host application may be identical to the first legacy host application; and

forwarding the revised second log-on message to the second legacy host application for completing a secure sign-on thereto.